Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application.

Please cancel claims 1-4, 11, 14, 16, 23, 24, and 30, without prejudice.

Please add new claims 31-34.

Please amend claims 5-9, 12, 13, 18, 20-22, 25-27, and 29, as indicated below. Material to be inserted is in **bold and underline**, and material to be deleted is in ~~strikeout~~ or, if the deletion is of five or fewer consecutive characters or would be difficult to see, in double brackets [[ ]].

<u>Listing of Claims</u>:

1.   (Canceled)

2.   (Canceled)

3.   (Canceled)

4.   (Canceled)

5.   (Currently Amended) The method of claim **31** [[1]], wherein the **adhesive label presents** ~~physical tag includes~~ a barcode that identifies the public key.

6.   (Currently Amended) The method of claim 5, wherein the **adhesive label presents** ~~barcode is formed as~~ a glyph code, and wherein the glyph code contains public-key identifying information in a machine-readable graphic.

7.   (Currently Amended) The method of claim **31** [[1]], wherein the **adhesive label presents** ~~physical tag carries~~ the public key.

8.   (Currently Amended) The method of claim **31** [[1]], wherein the **adhesive label** ~~physical tag~~ identifies a location on a digital storage medium, and wherein the location includes the public key.

9.   (Currently Amended) The method of claim **31** [[1]], further comprising sending the encrypted digital image from a sender to an address of a recipient, the address being identified by the **adhesive label** ~~physical tag~~.

10.   (Original) The method of claim 9, wherein sending includes transmitting a digital signature to the recipient, the digital signature being produced using a private key of the sender and relating to the digital image.

11.   (Canceled)

12.   (Currently Amended) The method of claim **31** [[11]], further comprising removing **an image portion corresponding to the adhesive label** ~~the digital tag~~ from the digital image before encrypting.

13.   (Currently Amended) A method of sending an encrypted image of a document, comprising:

disposing a physical tag on a document, the physical tag having a **glyph** code **with public-key identifying information** ~~that carries a public key~~;

digitizing the document to create a digital image that includes a digital representation of the **glyph** code;

Page 3 -   AMENDMENT
              Serial No. 10/086,771
              HP Docket No. 10015964-1
              KH Docket No. HPCB 334

reading the digital representation of the **glyph** code to obtain the public key;

encrypting the digital image with the obtained public key; and

sending the encrypted image to a recipient that holds a private key, the private

key forming an asymmetric public-private pair of cryptography keys with the public key.

14. (Canceled)

15. (Original) The method of claim 13, wherein the physical tag carries an address, the address corresponding to the recipient.

16. (Canceled)

17. (Original) The method of claim 13, wherein the physical tag is included on an adhesive label, and wherein disposing includes applying the adhesive label to the document.

18. (Currently Amended) A device for encrypting an image produced from spatially-distributed physical information, the device comprising:

at least one digitizing mechanism adapted to digitize spatially-distributed physical information to create a digital image, and to digitize a **glyph code** ~~physical tag~~ associated with the physical information ~~to create a digital tag~~, the **glyph code** ~~digital tag~~ being readable to identify a public key that is a public member of an asymmetric public-private pair of cryptography keys; and

a processor operatively connected to the digitizing mechanism and adapted to receive the digital image and **a digital representation of the glyph code** ~~digital tag~~ from the at least one digitizing mechanism, to read the **digital representation of the glyph code** ~~digital tag~~ to identify the public key, and to encrypt the image with the identified public key.

19.   (Original) The device of claim 18, wherein the physical information is included in a document, the document having a substrate that supports the physical information.

20.   (Currently Amended) The device of claim 19, wherein the **glyph code is presented by** ~~physical tag is included on~~ a label that is applied to the document, ~~the label having a code that identifies the public key~~.

21.   (Currently Amended) The device of claim 18, wherein the at least one digitizing mechanism is a single mechanism that digitizes **both** the **glyph code and** ~~physical tag~~ ~~during digitizing~~ the physical information .

22.   (Currently Amended) The device of claim 18, wherein the **glyph code** ~~physical tag~~ carries an address of a recipient, and the processor is adapted to be connected to a network and to send the encrypted image to the address through the network.

23.   (Canceled)

24.   (Canceled)

25.   (Currently Amended)   The device of claim 18, wherein the **glyph code** ~~physical tag~~ carries the public key.

26.   (Currently Amended)   The device of claim 18, wherein the **glyph code** ~~physical tag~~ identifies a location on a digital storage medium, and wherein the location includes the public key.

27.   (Currently Amended)   A program storage device readable by a processor, tangibly embodying a program of instructions executable by the processor to perform method steps for encrypting an image produced from physical information, comprising:

digitizing spatially-distributed physical information to create a digital image of the information;

digitizing a **glyph code** ~~physical tag~~ associated with the physical information ~~to create a digital tag, the digital tag being~~ **and** readable to identify a public key that is a public member of an asymmetric public-private pair of cryptography keys;

reading **a digital representation of the glyph code produced by digitizing the glyph code** ~~the digital tag~~ to identify the public key; and

encrypting the digital image with the identified public key.

28.   (Original)   The program storage device of claim 27, wherein the physical information is included in a document, the document having a substrate that supports the physical information.

29.   (Currently Amended)   The program storage device of claim 28, wherein the **glyph code is presented by** ~~physical tag is included on a~~ **an adhesive** label that is **affixed** ~~applied~~ to the document.

30. (Canceled)

31. (New) A method of encrypting a document, comprising:

affixing an adhesive label to a document, the adhesive label being optically readable to identify a public key that is a public member of an asymmetric public-private pair of cryptography keys;

digitizing the document after the step of applying to create a digital image of the document and the adhesive label;

identifying the public key using the digital image; and

encrypting at least a portion of the digital image with the identified public key.

32. (New) The method of claim 31, wherein the adhesive label is associated with a label carrier prior to affixing, further comprising separating the adhesive label from the label carrier before affixing the adhesive label to the document.

33. (New) The method of claim 32, wherein separating includes peeling the adhesive label off of the label carrier.

34. (New) The method of claim 13, wherein disposing a physical tag includes disposing a physical tag having a glyph code that includes a logo.